

# Researchers Say Sharing Is the Key to Privacy for EPC Tags

Three computer scientists say they have devised a means of protecting tag data by using a method that disperses pieces of a decryption key among multiple RFID tags.

By Mary Catherine O'Connor

Feb. 14, 2008—Three technologists have developed a process that they think can protect tag data and address consumers' privacy concerns without derailing existing efforts to integrate RFID throughout the supply chain. Ravi Pappu, cofounder and head of [ThingMagic](#)'s Advanced Development Group, Ari Juels, principal research scientist at [RSA Laboratories](#) (the research center of computer security firm [RSA](#)) and Bryan Parno, a graduate student at [Carnegie Mellon University](#), have published a paper describing their proposed approach to EPC data privacy protection. The technologists presented their findings at a recent RFID security workshop at [Johns Hopkins University](#).

The scheme is based on what is known as a threshold or secret-sharing cryptography, which uses a secret key to encrypt a number, then splits that key into multiple shares. The party attempting decryption must collect a specific number of those shares to figure out the key. The three researchers have dubbed their approach privacy-through-dispersion.

The major thrust of the research behind this approach has been in finding a means of shrinking the size of the key shares. Since secret-sharing cryptography has, thus far, been deployed only in applications where the memory size of each key share could be upwards of 128 bits—greatly exceeding the memory available on an EPC tag for this function—the researchers needed to find a method for boiling down each share's bit size. The technologists believe privacy-through-dispersion could be implemented to protect data encoded to EPC Gen 2 UHF passive tags without requiring any changes to the Gen 2 standard, and with just a firmware upgrade to Electronic Product Code (EPC) readers.

The EPC Gen 2 air-interface protocol allows for the use of a password to protect data encoded to a tag from being altered by an unauthorized party. The password, however, does not prevent the tag data from being interrogated by any EPC Gen 2 reader. That makes the protocol's kill command the only means of ensuring an EPC Gen 2 tag won't be read by an unauthorized party. But the problem with the kill command, Pappu says, is obvious: It kills the tag. This negates any value the tag holds in terms of authenticating a product warranty, return or exchange.

The approach Pappu and his collaborators have developed is predicated on a critical premise: that as a tagged product moves through the supply chain, its proximity to other tagged products of its ilk decreases. Let's take a single unit of a name-brand shaving razor, for instance, and call it Item A. At the manufacturer's facility, Item A is tagged and packed into a case carrying many other identical tagged razors; the case is then packed onto a pallet carrying multiple cases of this same product. At a distribution center, the pallet is broken down, and the case carrying Item A is shipped to a single store location. There, the case is stored in the back room until Item A is placed on a store shelf, along with a handful of other, identical and tagged units. Once Item A

is purchased, it is carried out of the store—thus, it goes from being in the company of many other identical tagged razors to, most likely, being completely isolated from others.

In secret sharing, the only means of decrypting a code—which, in this scenario, would be an EPC—is by collecting an adequate number of shares of the key needed for decryption. "You take a secret key, and you share the secret key such that if you have less than, say, 10 of the shares, you cannot recover the secret key," Pappu explains. "It is similar to the scenario in which you are trying to launch a missile, but you need five generals out of a total of seven generals to be present before you can launch."

Using the privacy-through-dispersion model, the EPC encoded to Item A's tag—and all of the other razors with which it would have been shipped—would have been encrypted early in the supply chain: after Item A was packed into a case, and before that case left the manufacturer's case-packing facility. "Encryption, in this system, is a bulk operation," Juels states. "[That is], it is applied to clusters of objects, and not to objects individually." He adds, however, that there is some flexibility to add or remove individual tags from the cluster without disrupting the ability to decrypt individual tags.

The key needed to decrypt any EPC in a case of tagged items would be split it up among the tags attached to other units packed in the same case. The software required to encrypt and decrypt the EPCs would reside on interrogators used to encrypt and decrypt the tags. To encrypt the tags, the software would use algorithms to create a key and then assign shares of that key to a pre-set number of EPCs in the tag population. To decrypt any of the encrypted tags, the reader would need to either collect or have access to, through a network connection, enough key shares to generate the whole key—again, using algorithms in the software. According to Pappu, upgrading readers with firmware enabling them to encrypt and decrypt the tag is the only change users of EPC technology in the supply chain would require—but each party that ships or receives tagged goods would need the software, and the algorithms it contains, to decrypt the EPCs.

Upon receiving the case containing Item A at its loading dock, the store would read all of the tags within the case and, thereby, capture the required number of shares to decrypt them all, including Item A's tag. The number of shares required to deduce the key and use it to decrypt any tag would be lower than the total number of shares in the case, Ravi says. This way, the failure to read a few of the tags within a case—due to RF interference or some other problem—would not limit the receiver's ability to attain the key.

Once the case is received at a store, any interrogator connected to the store network would have access to the key needed to decrypt the tag on Item A, or on any other tag shipped in the same case, enabling store employees to perform shelf-level inventory or read the EPC at the point of sale (or on a return).

Without encrypting the EPC encoded to Item A, Shopper A would walk out of the store and (assuming Item A's tag had not been killed at the point of sale) anyone with an EPC Gen 2 reader would be able to read the tag and, by comparing it with a database of EPCs and the product information associated with those EPCs, figure out that Shopper A had purchased the razor. This could easily be accomplished without Shopper A's knowledge, thereby violating that person's assumed privacy. But if the EPC encoded to the tag had been encrypted using the proposed scheme, the snoop wouldn't be able to read the tag without also reading enough tags on the razors shipped along with Item A to complete the key needed to decrypt Item A's EPC. And because most of those other tags would be located in the back of the store, in a secured area, it would be extremely difficult for an unauthorized person to access them.

Most likely, Shopper A wouldn't care whether someone could determine, by reading an unencrypted EPC, that he or she was carrying a new razor blade. But there are other products—such as OxyContin, Viagra or certain other pharmaceutical items—about which a person might feel much more guarded, and prefer to keep private.

Pappu and Juels say they hope to arrange for the first real-world tests of privacy-through-dispersion to be

conducted on a pharmaceutical product, in a closed-loop supply chain. The privacy-through-dispersion model is irrelevant for drugs shipped in bulk containers to pharmacies, where they are dispensed in smaller bottles to fill prescriptions. However, it might be useful for tags applied at the item level to medicines shipped through a supply chain, although it's uncertain at this point if such tags would be encoded with any data that could be easily used to identify the drugs.

RELATED\_ARTICLES "[The privacy-through-dispersion approach] can't be adopted overnight, but our vision is to find opportunities to try it out and see the value," Pappu says. Both ThingMagic and RSA have filed patents on privacy-through-dispersion, and Pappu says ThingMagic may eventually commercialize the software enabling the data protection scheme. The paper describing the elemental tenets of privacy-through-dispersion has been published [here](#), on the Web site of the [International Association for Cryptologic Research](#), and is currently under peer review.

In addition, Pappu and Juels note that manufacturers could employ privacy-through-dispersion encryption to help authenticate their products as they move through the supply chain, by sharing the secret key among tags applied to the many cases that make up shipments. If, for instance, 10 cases are supposed to be enough to get the key, and a system fails to collect an adequate number of shares after it reads the EPCs from 10 cases, then a company could assume there are some counterfeit tags (and possibly counterfeit products) within those cases, Pappu says.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved